

REMARKS

Claims 1-27 were pending in the application. The pending claims stand rejected. Claim 24-25 have been cancelled herein, thereby rendering moot the section 101 rejection with respect to these claims. Assignee traverses the rejections of the claims.

Claim Rejections – 35 U.S.C. § 102

The pending claims stand rejected under 35 U.S.C. § 102(e) as being anticipated over US 2005/0015583 (Sarkkinen). These rejections are traversed.

In rejecting claim 1, the office action maintains that Sarkkinen discloses the features of claim 1. For example, the office action maintains that paragraphs 22-26 of Sarkkinen disclose that a broadcast key is generated on the user device and that the generated broadcast key is sent from the user device over a network as recited in claim 1. These paragraphs of Sarkkinen read as follows (emphasis added):

[0022] Moreover, the invention proposes a *user entity* in a network which is adapted to *receive an encrypted multicast message* transmitted to a plurality of user entities in a network by using a multicast service, and to decrypt the encrypted multicast message by using deciphering.

[0023] Furthermore, the invention also proposes a network comprising a multicast service control device described above and at least one user entity described above.

[0024] Further advantageous developments are set out in the dependent claims.

[0025] In particular, the encrypted multicast message may be decrypted in each user entity individually.

[0026] The ciphering may be performed by using a ciphering key, wherein the ciphering key may be the same for encrypting and decrypting, or a first ciphering key may be used for encrypting whereas a second ciphering key different from the first ciphering key may be used for decrypting.

These passages from Sarkkinen teach that a user entity can process a received encrypted multicast message using a ciphering key. However, there is no disclosure in these passages of

generation of a broadcast key (as required in claim 1), only utilization of a ciphering key to process a message. Additionally, these passages are discussing how a message *received by a user entity* is to be processed, whereas claim 1 recites that information (i.e., a generated broadcast key) is *sent from the user device*. There is no disclosure whatsoever in these paragraphs of Sarkkinen of sending from the user device information such as a generated broadcast key.

Still further, assignee respectfully disagrees with the office action that paragraphs 29, 46, and 166-167 of Sarkkinen disclose the last paragraph of claim 1 and with the interpretation by the office action of the phrase “joining/activation of the transmission” that appears in paragraph 29. These paragraphs and the phrase that appears in paragraph 29 are directed to cipher key generation and the information sent to the user entity to perform such generation. They provide no disclosure of a broadcast key (that is sent from a user device) to indicate that multicast content is to be provided to the user device. For example, the phrase specially mentioned by the office action, when read in its complete context, relates to the transmission of ciphering key generation related input parameters to a user entity. (See, also paragraph 28 of Sarkkinen for additional context and details of these parameters and their transmission to a user entity.) After consideration of the complete context of the disclosure in Sarkkinen, it is clearly evident that this phrase is not discussing at all a broadcast key (that has been sent from the user device) for indicating that multicast content is to be provided to the user device as required by claim 1. Because of such lack of disclosure in Sarkkinen, claim 1 is allowable and should proceed to issuance.

Assignee respectfully disagrees with other positions in the office action. For example, assignee disagrees with the rejection of dependent claim 21. Claim 21 recites that the user

device accesses different multicast services of a provider by providing different broadcast keys to the provider, and that the different broadcast keys are generated on the user device. The office action maintains that paragraphs 150 and 271 of Sarkkinen disclose the last limitation of claim 21 (i.e., different broadcast keys are generated on the user device). Paragraphs 150 and 271 of Sarkkinen read as follows:

[0150] When using SIM for storing the security information, it is advantageous to increase the SIM card storage capacity in order to store all necessary decryption keys and parameters, since currently this storage capacity is e.g. 8 kB or 16 kB.

[...]

[0271] Joining is proposed to be performed before each session of the service (i.e. if a user wants to receive 4 news clips per day, he has to perform joining also 4 times/day), which means--depending on the number of supported MBMS services in UE--a frequent activation of the joining request messages and continuous establishment of the RRC connection or RRC state change transactions is necessary

These paragraphs of Sarkkinen clearly provide no disclosure of generation of a broadcast key, let alone that different broadcast keys are generated on the user device. Because of such lack of disclosure in the cited reference, claim 21 is allowable for this additional reason and should proceed to issuance.

With respect to the other independent claims, claims 26 and 27 recite similar limitations as claim 1. Accordingly, for the reasons provided above with reference to claim 1, the other independent claims are also allowable over the cited references, and should proceed to issuance.

Assignee at this time has not provided arguments in support of the patentability of certain dependent claims. It is respectfully submitted that because the independent claims are now in condition for allowance, the dependent claims which depend directly or indirectly therefrom are also in condition for allowance. However, assignee reserves the right to argue the patentability of certain of the dependent claims in the instant application at a future time, should that become necessary.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issue.

Respectfully Submitted,

JONES DAY


John V. Biernacki (Reg. No. 40,511)
Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216-586-7747)